Page 3692 - 3701 **DOI:** *https://doij.org/10.10000/IJLMH.1111953*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 2

2026

A Critical Analysis of Judicial Role in Strengthening Digital Privacy in India

ANBARASI. M[1] AND DR. S. JENIFER STELLA[2]

ABSTRACT

This chapter examines the important role played by the judiciary in strengthening digital privacy in India. In the absence of a detailed legal framework in earlier times, the courts played a key role in protecting individual rights and shaping privacy law. A major development came with the landmark decision in Justice K.S. Puttaswamy v Union of India, where the Supreme Court recognised the right to privacy as a fundamental right under Article 21 of the Constitution.[1] This judgment laid the foundation for the protection of digital privacy in India. The chapter further analyses how judicial decisions have addressed issues such as surveillance, misuse of personal data, and the need for data protection. It also explains how the judiciary balances individual privacy with state interests like national security. However, challenges such as weak enforcement and rapid technological changes still exist. Overall, the chapter highlights that judicial intervention remains essential for ensuring effective digital privacy protection in India.

Keywords: *Digital Privacy, Judiciary, Fundamental Rights, Article 21, Data Protection, Surveillance, Constitutional Law, Personal Data, Privacy Rights, India*

I. INTRODUCTION

The protection of digital privacy in India has largely developed through judicial intervention, especially during the early stages when there was no strong and comprehensive legal framework. While laws relating to data protection have gradually evolved, the judiciary has played a major role in interpreting constitutional provisions and expanding the scope of fundamental rights. Through its decisions, courts have helped establish important legal principles to protect individual privacy in the digital age. In the Indian legal system, the judiciary acts as the guardian of fundamental rights and ensures that both state actions and laws follow constitutional values. Over time, the courts have taken a progressive approach by expanding the meaning of the right to life and personal liberty under Article 21 to include the right to privacy. This development has been significant in addressing new challenges arising

[1] Author is an LL.M. Student at Vels Institute of Science, Technology & Advanced Studies, Chennai, Tamil Nadu, India.
[2] Author is an Assistant Professor & Hod School of Law, Vels Institute of Science, Technology & Advanced Studies, Chennai, Tamil Nadu, India.

 [ISSN 2581-5369]

from technological growth and digital data usage. With the increasing use of the internet, social media, and digital platforms, privacy concerns have shifted from physical intrusion to the protection of personal data and informational privacy. As a result, the judiciary's role has become even more important in safeguarding individuals against misuse of their data by both government and private entities. A major turning point in this area came with the landmark judgment in Justice K.S. Puttaswamy (Retd.) v. Union of India, where the Supreme Court recognized privacy as a fundamental right under Article 21. This judgment laid a strong foundation for the protection of digital privacy and influenced future legal developments. Following this, courts have also addressed issues such as surveillance, data collection, and unauthorized sharing of personal information, emphasizing the need for transparency, accountability, and procedural safeguards. The judiciary has further contributed by highlighting the importance of a strong data protection system, which eventually led to the enactment of the Digital Personal Data Protection Act 2023. At the same time, courts must balance privacy with other important concerns like national security and public interest. They apply principles such as legality, necessity, and proportionality to ensure that privacy rights are not violated unnecessarily. Despite its important role, the judiciary faces challenges such as rapid technological changes, complex data systems, and limited legislative clarity in certain areas. This chapter, therefore, examines how the judiciary has strengthened digital privacy in India, focusing on key judgments, evolving legal principles, and the need for stronger safeguards in the future.

II. JUDICIAL RECOGNITION OF PRIVACY AS A FUNDAMENTAL RIGHT

The recognition of privacy as a fundamental right in India has developed mainly through judicial interpretation. In the beginning, the Constitution did not clearly mention the right to privacy, and courts were hesitant to recognize it. In early cases like M.P. Sharma v. Satish Chandra[3] and Kharak Singh v. State of Uttar Pradesh, the Supreme Court denied that privacy was a fundamental right. However, over time, the judicial approach changed. In Gobind v. State of Madhya Pradesh, the Court accepted that privacy could be part of personal liberty under Article 21, though it could be limited in certain situations. This marked the beginning of a broader understanding of privacy.[4] The scope of Article 21 was further expanded in Maneka Gandhi v. Union of India, where the Court held that the right to life and personal liberty must be interpreted in a wide and meaningful way. Later decisions such as R. Rajagopal v. State of Tamil Nadu and People's Union for Civil Liberties (PUCL) v. Union of India recognized

[3] *M.P. Sharma v Satish Chandra AIR 1954 SC 300 (India)*
[4] *Gobind v State of Madhya Pradesh (1975) 2 SCC 148 (India).*

 [ISSN 2581-5369]

specific aspects of privacy, including protection against unauthorized publication and telephone tapping.[5] A major turning point came with the landmark judgment in Justice K.S. Puttaswamy (Retd.) v. Union of India, where the Supreme Court clearly declared that privacy is a fundamental right under Article 21.[6] The Court also explained that privacy includes personal autonomy, dignity, and protection of personal data. It introduced principles such as legality, necessity, and proportionality to test any restriction on privacy. Overall, the judiciary has played a key role in transforming privacy from a denied right into a well-recognized fundamental right. This development has become especially important in the digital age, where protection of personal information is essential.

Analysis of Landmark Judgments on Digital Privacy

The development of digital privacy in India has been strongly influenced by important judicial decisions. Courts have played a key role in applying constitutional principles to modern issues such as data protection, surveillance, and use of technology. One of the most important cases is Justice K.S. Puttaswamy (Retd.) v. Union of India, where the Supreme Court not only recognized privacy as a fundamental right but also explained the idea of informational privacy. The Court stated that individuals must have control over their personal data and introduced the threefold test of legality, necessity, and proportionality to check any interference with privacy. This principle was further applied in K.S. Puttaswamy (Aadhaar-5J.) v. Union of India, where the Court examined the Aadhaar system. While the scheme was upheld, the Court placed limits on data sharing and restricted access by private entities. This shows that the judiciary supports the use of technology but insists on proper safeguards to prevent misuse of personal information. Another important judgment is Anuradha Bhasin v. Union of India, which dealt with internet shutdowns. The Court held that access to the internet is important for exercising fundamental rights and that restrictions must be reasonable and proportionate. Similarly, in Shreya Singhal v. Union of India, the Court struck down a law that allowed arbitrary control over online communication, thereby protecting both freedom of expression and digital privacy. Earlier cases like District Registrar and Collector v. Canara Bank and People's Union for Civil Liberties (PUCL) v. Union of India also contributed by recognizing the need to protect personal and communication data from unlawful interference. A critical analysis of these judgments shows that the judiciary has tried to balance privacy with public interests such as national security and welfare. It has also filled gaps where detailed laws were missing. However, challenges remain

[5] *R Rajagopal v State of Tamil Nadu (1994) 6 SCC 632 (India).*
[6] *Justice KS Puttaswamy (Retd.) v Union of India (2017) 10 SCC 1 (India).*

 [ISSN 2581-5369]

due to rapid technological changes and the lack of comprehensive legal frameworks. Overall, these judgments highlight the important role of courts in strengthening digital privacy in India, while also showing the need for strong legislation to support judicial efforts.

III. ROLE OF THE JUDICIARY IN STRENGTHENING DATA PROTECTION

The judiciary in India has played a very important role in strengthening data protection, especially during the time when there was no clear and comprehensive law on the subject. With the rapid growth of digital technology, personal data began to be collected and used on a large scale. In this situation, courts stepped in to protect the rights of individuals by interpreting the Constitution in a broader and more meaningful way. Through its decisions, the judiciary not only recognized privacy as a fundamental right but also laid down important principles that guide data protection in India today. One of the most significant contributions of the judiciary is the recognition of informational privacy as a part of the right to privacy. This was clearly established in Justice K.S. Puttaswamy (Retd.) v. Union of India, where the Supreme Court held that personal data is closely connected to an individual's dignity and autonomy. The Court observed that in a digital society, people constantly share information through online platforms, making them vulnerable to misuse. By recognizing informational privacy, the judiciary created a strong foundation for modern data protection laws in India. Another important contribution of the judiciary is the development of constitutional principles to regulate data protection. In the same case, the Court introduced the threefold test of legality, necessity, and proportionality. According to this test, any action that interferes with privacy must be supported by law, must have a legitimate purpose, and must be proportionate to that purpose. This principle is now widely used to evaluate the validity of data collection and surveillance practices. It ensures that state authorities do not misuse their power while handling personal data. The judiciary has also played a key role in highlighting the need for proper legislation on data protection. In the Puttaswamy judgment, the Supreme Court clearly stated that India requires a strong legal framework to regulate the collection and use of personal data. This observation influenced the development of policies and ultimately contributed to the enactment of the Digital Personal Data Protection Act 2023. The courts, therefore, have not only interpreted the law but have also guided the legislative process. In addition to influencing law-making, the judiciary has actively intervened to prevent misuse of personal data. In K.S. Puttaswamy (Aadhaar-5J.) v. Union of India, the Supreme Court examined the Aadhaar scheme, which involved the collection of biometric data. While the Court allowed the scheme, it imposed important restrictions to protect privacy. It limited the use of Aadhaar data and restricted access by private companies.

 [ISSN 2581-5369]

This shows that the judiciary supports digital development but insists on strong safeguards to prevent misuse of personal information.The judiciary has also developed procedural safeguards to prevent arbitrary state actions. In People's Union for Civil Liberties (PUCL) v. Union of India, the Court laid down guidelines to regulate telephone tapping. It emphasized the need for proper authorization and oversight to ensure that surveillance does not violate individual privacy.

These principles continue to be relevant today, especially in the context of digital surveillance technologies. Another important case is Anuradha Bhasin v. Union of India, where the Court dealt with internet shutdowns. The Court held that restrictions on internet access must be reasonable, proportionate, and subject to judicial review. Although the case mainly focused on freedom of expression, it also highlighted the importance of digital access in protecting privacy and personal autonomy.[7] The judiciary has further recognized that data protection is not only about controlling state actions but also about regulating private entities. In today's digital world, private companies collect and process large amounts of personal data. The courts have emphasized that the state has a duty to ensure that such companies do not misuse personal information. This shows that data protection extends beyond government actions and includes safeguarding individuals from private misuse as well. Moreover, the judiciary has promoted a rights-based approach to data protection. It has stressed that data protection is closely linked to fundamental values such as dignity, autonomy, and informed consent. By doing so, the courts have ensured that data protection is treated not just as a technical or regulatory issue, but as a matter of fundamental rights. This approach is in line with global standards and strengthens India's legal framework. However, the role of the judiciary also has certain limitations. Courts usually decide cases based on specific facts, which may lead to differences in interpretation. In addition, modern technologies such as artificial intelligence and big data are complex and constantly evolving, making it difficult for courts to keep up with new challenges. The judiciary also depends on the legislature to create detailed and effective laws. Without proper implementation by the government, judicial decisions alone may not be sufficient. Despite these challenges, the judiciary has made a significant contribution to strengthening data protection in India. It has expanded the scope of fundamental rights, introduced important legal principles, and influenced the creation of modern laws. In conclusion, the judiciary continues to play a crucial role in ensuring that data protection in India develops in a way that respects

[7] *Anuradha Bhasin v. Union of India, (2020) 3 S.C.C. 637 (India).*

 [ISSN 2581-5369]

constitutional values and protects the rights of individuals in the digital age.

IV. EMERGING LEGAL ISSUES IN DIGITAL PRIVACY

The fast growth of digital technology has created new challenges for protecting privacy. Even though India has introduced laws like the Digital Personal Data Protection Act 2023, technology is developing much faster than legal rules. Because of this, many new legal issues have emerged that require attention from both courts and lawmakers. One major issue is the use of artificial intelligence (AI) and automated decision-making systems. These systems depend on large amounts of data to make decisions. While they are useful, they can also lead to problems such as unfair profiling and discrimination.

Many AI systems are not transparent, which makes it difficult for individuals to understand how their data is used or how decisions are made about them. This raises serious concerns about accountability and fairness. Another important issue is mass surveillance. Governments use advanced technologies for security and law enforcement, but excessive surveillance can violate individual privacy.

In Justice K.S. Puttaswamy (Retd.) v. Union of India, the Supreme Court emphasized that privacy is a fundamental right and must be protected from unnecessary state interference. This highlights the need for clear legal safeguards and proper oversight to prevent misuse of surveillance powers. Big data analytics is also creating new challenges. Organizations collect and analyse large amounts of data to understand patterns and behaviour. While this has benefits, it can also reveal personal information even from data that appears harmless. This makes it difficult to clearly separate personal and non-personal data and increases the risk of privacy violations. Data breaches and cybersecurity threats are another growing concern. As more services become digital, personal data is stored online and becomes vulnerable to hacking and unauthorized access. Data breaches can cause serious harm, including financial loss and identity theft. Although laws require companies to protect data, constant updates are needed to deal with new cyber threats. Cross-border data transfer is also a complex issue. Data often moves between countries, which creates problems related to jurisdiction and enforcement of laws. While Indian law allows data transfers under certain conditions, there is still uncertainty about how to ensure proper protection when data leaves the country. The role of private companies in handling data has also increased. Many technology companies collect large amounts of personal information for business purposes such as advertising and analysis. This concentration of data raises concerns about misuse and lack of user control. Therefore, it is important to ensure that private entities are also held accountable under data protection laws. Another challenge is the concept

 [ISSN 2581-5369]

of consent. In theory, individuals must give permission before their data is used. However, in practice, people often agree to long and complex privacy policies without fully understanding them. This problem, known as "consent fatigue," reduces the effectiveness of consent as a tool for protecting privacy. Emerging technologies like the Internet of Things (IoT) also create risks.

V. CHALLENGES IN ENFORCEMENT OF DATA PROTECTION LAWS

The success of any data protection law depends not only on strong rules but also on how well those rules are enforced. In India, even after recognizing privacy as a fundamental right and introducing the Digital Personal Data Protection Act 2023, many challenges still affect proper enforcement. These challenges arise due to institutional limits, technical difficulties, lack of awareness, and the fast-changing nature of digital technology. One major challenge is the limited capacity of regulatory authorities. The establishment of the Data Protection Board of India is an important step, but its effectiveness depends on having enough resources, independence, and technical knowledge. With increasing data breaches and large-scale data processing, it may be difficult for the Board to handle all cases efficiently. Another issue is the lack of coordination between different regulatory bodies.

India has multiple authorities such as sector regulators and technical agencies, which can sometimes lead to overlapping responsibilities and confusion. This may result in delays and inconsistent enforcement of data protection laws. The rapid growth of technology also creates difficulties in enforcement. Technologies like artificial intelligence, cloud computing, and big data are complex and require specialized knowledge. Courts and regulators may find it challenging to fully understand these systems, which can affect their ability to make effective decisions. Cross-border data transfer is another important concern. Personal data often moves across countries, making it difficult to determine which laws apply and how they should be enforced. Although Indian law allows such transfers under certain conditions, the lack of strong international cooperation can limit enforcement. Lack of public awareness is also a serious problem. Many people do not fully understand how their data is collected or what rights they have. This reduces their ability to take action when their privacy is violated, weakening the overall effectiveness of the law. In addition, grievance redressal mechanisms are not always strong enough. Delays, complex procedures, and limited accessibility can discourage individuals from filing complaints. This affects the protection available to data users. Ensuring compliance by private companies is another major challenge. Many large companies collect and process huge amounts of personal data. Monitoring their activities and ensuring that they follow the law can be difficult for regulators, especially when these companies operate across different

 [ISSN 2581-5369]

countries. Finally, the lack of uniform compliance standards makes enforcement more difficult. Different organizations follow different practices, which creates inconsistency. Without clear standards, it becomes harder for authorities to monitor compliance and impose penalties. In conclusion, although India has developed a strong legal framework for data protection, effective enforcement remains a challenge. Issues such as limited institutional capacity, technological complexity, lack of awareness, and government exemptions need to be addressed. Strengthening enforcement mechanisms is essential to ensure better protection of digital privacy and to build trust in the digital system.

VI. NEED FOR STRONGER LEGAL SAFEGUARDS

The rapid growth of digital technologies has made the protection of personal data more important than ever. In India, important progress has been made with the recognition of privacy as a fundamental right and the introduction of the Digital Personal Data Protection Act 2023. However, the current legal framework still has gaps, and stronger safeguards are needed to deal with new challenges in the digital environment. One key requirement is a more comprehensive and detailed legal framework. While the present law provides basic rules for data protection, it does not fully address issues such as artificial intelligence, automated decision-making, and non-personal data. As technology continues to evolve, laws must also expand to cover these new areas and ensure that all types of data processing are properly regulated. Another important area is the strengthening of individual rights. At present, individuals have rights such as access, correction, and erasure of their data. However, additional rights like data portability and the right to object to automated decisions are not fully developed. Expanding these rights would give individuals more control over their personal information and bring India closer to global standards. The concept of consent also needs improvement. In many cases, individuals agree to privacy policies without fully understanding them.

This makes consent less effective as a protective tool. Stronger safeguards are needed to ensure that consent is clear, informed, and voluntary. Simplifying privacy notices and focusing on accountability of organizations can help improve this situation.Regulation of state surveillance is another critical issue.

VII. FINDINGS

1. In India, the right to privacy has been judicially recognized as a fundamental right under Article 21 of the Constitution.

 [ISSN 2581-5369]

2. The landmark judgment in Justice K.S. Puttaswamy (Retd.) v. Union of India significantly expanded the scope of privacy to include informational and digital privacy.
3. The judiciary has played a crucial role in strengthening digital privacy by:

- Expanding the scope of fundamental rights
- Establishing principles such as legality, necessity, and proportionality

4. Judicial decisions have addressed key issues such as:

- Surveillance and data collection
- Internet access and digital freedoms
- Protection against arbitrary state action

VIII. SUGGESTION

The study suggests that India's data protection system needs continuous improvement to effectively deal with modern digital challenges. Although the judiciary has played an important role in protecting privacy, stronger legal and institutional support is necessary to make these protections more effective in practice. One important suggestion is to strengthen the existing legal framework, especially the Digital Personal Data Protection Act 2023. The law should be expanded to clearly regulate emerging areas such as artificial intelligence, automated decision-making, and big data. be made more accountable for how they collect and use data, rather than relying only on user consent. The principles laid down in Justice K.S. Puttaswamy (Retd.) v. Union of India—legality, necessity, and proportionality—must be strictly followed in all cases involving data collection and monitoring. Independent oversight mechanisms should also be introduced to prevent misuse of surveillance powers. Finally, the judiciary must continue to play an active role in protecting privacy. Through continuous interpretation of laws and application of constitutional principles, courts can ensure that digital privacy remains a protected fundamental right even as new challenges emerge.

IX. CONCLUSION

The role of the judiciary in strengthening digital privacy in India has been highly important and transformative. In the early stages, when there was no clear constitutional provision or detailed law on privacy, the judiciary took an active role in protecting individual rights. Through progressive interpretation of the Constitution, courts expanded the meaning of the right to life and personal liberty to include privacy, especially in the context of growing digital technologies. A major turning point came with the judgment in Justice K.S. Puttaswamy (Retd.) v. Union of

 [ISSN 2581-5369]

India, where the Supreme Court clearly recognised privacy as a fundamental right. This decision established that privacy is closely linked to dignity, autonomy, and individual freedom. It also created a strong constitutional base for protecting personal data in the digital age and influenced later legal and policy developments. The judiciary has also developed key principles for protecting privacy, especially the doctrine of proportionality. According to this principle, any restriction on privacy must be lawful, necessary, and proportionate to the objective. This framework is now widely used to examine issues like surveillance, data collection, and digital governance, ensuring that state actions do not violate individual rights without proper justification. Another major contribution of the judiciary is highlighting the need for strong data protection laws. Observations made in the Puttaswamy case about informational privacy influenced the creation of the Digital Personal Data Protection Act 2023. This shows how judicial decisions can guide legislative development and strengthen the overall legal system. At the same time, courts have carefully handled the balance between national security and privacy. They have recognised that while security is important, it should not come at the cost of fundamental rights. By insisting on safeguards and judicial review, the judiciary ensures that government actions remain within constitutional limits. In conclusion, the judiciary has played a central role in shaping digital privacy law in India. Through progressive judgments, it has expanded fundamental rights, created important safeguards, and influenced legislation. However, protecting privacy in the digital age requires a combined effort from the judiciary, legislature, and executive. Only through strong laws, effective enforcement, and continued judicial vigilance can the right to privacy be fully protected in an evolving technological world.

*****

 [ISSN 2581-5369]